Countering Denial-of-Service Attacks in Network-based Control Systems

prof.dr.ir. Geert Deconinck, dr. Hakem Beitollahi, KU Leuven, EnergyVille, Leuven, Belgium

Summary

Network-based control systems are at the heart of critical infrastructures. However, remotely supervised or controlled systems are open to denial of service attacks. Four architectures are presented to mitigate the effects of such cyberattacks. FOSEL combines overlay techniques with filtering to reduce the effect of such attacks. A cooperative defense technique relies on intermediate routers to move the defense area to the source away from the attacked target. The Ferris wheel is a ring based onion circuit for hidden services. Finally ConnectionScore provides a way to detect denial of service attacks from abnormal behaviour. Simulation and experimental results underpin the suitability of these approaches to reduce the impact of denial of service attacks on network based control systems.

1 References

[1] H. Beitollahi, G. Deconinck, “A Dependable Architecture to Mitigate Distributed Denial of Service Attacks in Network-Based Control Systems,” Int. Journal of Critical Infrastructure Protection (Elsevier), Vol. 4, No. 3-4, Dec. 2011, p. 107-123. http://dx.doi.org/10.1016/j.ijcip.2011.06.003

[2] H. Beitollahi, G. Deconinck, “Ferris Wheel: A Ring Based Onion Circuit for Hidden Services,” Int. Journal of Computer Communications (Elsevier), Vol. 35, Iss. 7, Apr. 2012, p. 829-841. http://dx.doi.org/10.1016/j.comcom.2012.01.008

[3] H. Beitollahi, G. Deconinck, “Tackling Application-layer DDoS Attacks,” Procedia Computer Science (Elsevier), Vol. 10, 2012, pp. 432-441. http://dx.doi.org/10.1016/j.procs.2012.06.056

[4] H. Beitollahi, G. Deconinck, “A Four-Step Technique for Tackling DDoS Attacks,” Procedia Computer Science (Elsevier), Vol. 10, 2012, pp. 507-516. http://dx.doi.org/10.1016/j.procs.2012.06.065

[5] H. Beitollahi, G. Deconinck, "A Ring Based Onion Circuit for Hidden Services," Chapter in P. Laud (Ed.), “Information Security Technology for Applications”, ISBN 978-3-642-29614-7, Lecture Notes in Computer Science LNCS Vol. 7161, Springer-Verlag, Berlin, Germany, May 2012, pp. 13-30. http://dx.doi.org/10.1007/978-3-642-29615-4_3

[6] H. Beitollahi, G. Deconinck, “Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks,” Int. Journal of Computer Communications (Elsevier), Vol. 35, Iss. 11, Jun. 2012, p. 1312-1332. http://dx.doi.org/10.1016/j.comcom.2012.04.008

2 Biographies

Prof.dr.ir. Geert Deconinck is full professor at KU Leuven and head of the research unit ESAT/Electa. His research interest focuses on the design and evaluation of dependable systems for industrial automation and control of electrotechnical applications. Examples include smart grids and distributed control of distributed energy resources. He teaches topics related to industrial automation, electrical installations, measurement techniques and smart grids. He is a fellow of IET and a senior member of IEEE. (geert.deconinck@esat.kuleuven.be)

Hakem Beitollahi obtained his PhD at the KU Leuven in 2012.